PRESIDIO®

SOLUTIONS BRIEF

Cybersecurity

Cloud Security Posture Assessment

THE CHALLENGE

At Presidio we understand the complex challenges that come with transitioning to the cloud and the importance of maintaining a strong security posture. Ensuring critical assets and sensitive data are protected in a dynamic environment provides a foundation for increased agility and innovation. It is imperative for organizations to implement and actively monitor secure cloud configurations, cloud activity, resource vulnerabilities, regulatory compliance, and risk management. The increasing reliance on cloud computing has amplified the need for effective security measures that can address these concerns and provide peace of mind for organizations as they continue to leverage the cloud to achieve their business goals.

THE SOLUTION

Presidio offers a comprehensive suite of highly advanced cybersecurity protections. Clients look to the Presidio Cloud Security Posture Assessment to understand their current cloud risk levels.

A Cloud Security Posture Assessment gives organizations a static security analysis of their Cloud environment(s) that aligns with the best practices of the Well Architected Framework's Security Pillars (AWS & Azure), and support National Institute of Standards and Technologies (NIST) and the Center for Internet Security Critical Security Controls (CIS) frameworks.

Focus Areas:

AWS	AZURE
AWS Security Best Practices based on the five (5) pillars of security which are Identity & Access Management (IAM), Detection, Infrastructure Protection, Data Protection, and Incident Response	Azure Security Best Practices based on the four (4) pillars of security which are Identity & Access Management (IAM), Infrastructure Protection, Data Protection, and Application Security
A high-level overview of the AWS account(s) architecture and what security guardrails are currently in place to help drive discussions	A high-level overview of your Azure subscription(s) architecture and what security guardrails are currently in place to help drive discussions

During the assessment, the Presidio team will engage with cloud security architects and key stakeholders through a discovery and review exercise. Presidio will also use an automated Cloud Security Posture Management (CSPM) tool to analyze the customers cloud environments. A report of findings and remediation recommendations will help develop a prioritized action plan.

Review compliance with leading security frameworks such as CIS, NIST CSF, CSA CCM, HIPAA, PCI-DSS, ISO-27001, SOC2 and others.

Findings & Recommendations

Presidio will work directly with the customer to give recommendations on tactical activities that could be changed now to make the environment more secure. Below are some example areas:

- Misconfiguration
- Identity & Access Management
- Logging
- Networking
- Sensitive Data exposure
- Cloud Activity anomalies

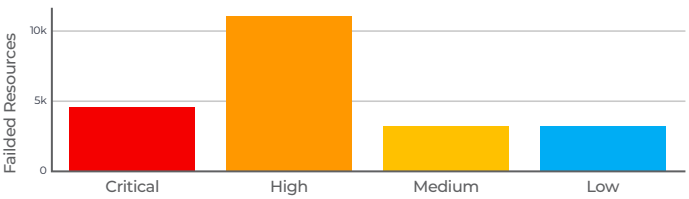
134 Total Containers with Critical Vulnerabilities

1636 Hosts with Critical Vulnerabilities

4576 Total Critical Cloud Compliance Findings

25 Total High / Critical Behaviors Detected

Compliance Severities Found



Sample Report

Cloud Security Posture Assessment

Detailed Findings & Recommendations are provided to identify top security concerns:

- **Findings Summary** with recommendations
- **Detail Findings Report(s)** showing the detail of the findings
- **Prioritized Actions List** to remediate security issues

The Cloud Security Posture Assessment is quick to execute (typically takes less than an hour to connect to the accounts and a couple of days for a final report) and provides comprehensive and immediately actionable results.

KEY BENEFITS

Clients need better insight about their security posture within their Cloud environment(s). Presidio clients will gain the confidence in their current position, and a prioritized roadmap for achieving the cybersecurity posture they need to protect their business. With a remediation plan, some immediate actions can resolve issues, while identification of gaps can help prioritizing investments when they are needed.

Example CSPA Finding

AWS: Eliminate use of the 'root' user for administrative and daily tasks

DESCRIPTION:

With the creation of an AWS account, a 'root' user is created that cannot be disabled or deleted. That user has unrestricted access to and control over all resources in the AWS account. It is highly recommended that the use of this account be avoided for everyday tasks.

SCORE:

Category: CIS AWS Foundations

Severity: Critical

RATIONALE:

The 'root' user has unrestricted access to and control over all account resources. Use of it is inconsistent with the principles of least privilege and separation of duties, and can lead to unnecessary harm due to error or account compromise.

RECOMMENDATIONS:

- Change the 'root' user password
- Deactivate or delete any access keys associated with the 'root' user
- Monitoring usage of the 'root' user can be accomplished by implementing recommendation 3.3 Ensure a log metric filter and alarm exist for usage of the 'root' user

WHAT MAKES US DIFFERENT

Presidio is a trusted partner to our clients, securing their infrastructure, employees, customers, and assets from ever-growing cyber threats. Our clients trust Presidio:

- **Holistic Cloud Security** – Presidio focuses on a holistic approach to cloud security. We partner with a broad spectrum of cyber vendors to secure the entirety of the cloud environment(s), from the infrastructure, through the network, and to the applications
- **Multi-cloud and Hybrid-cloud Capabilities** – Presidio has capabilities with the leading cloud providers and on-prem environments. Cloud security must be considered in the context of the entire organization. With deep knowledge of every layer of the IT, cloud, and cyber architecture, combined with proven methodologies Presidio can ensure customers are secure end-to-end

WHY PRESIDIO

Presidio is a leading digital systems integrator, with deep experience in networking, cloud computing and broad hybrid infrastructures. Presidio recognizes that cybersecurity is foundational to the success of any business and has a highly specialized expert team at the ready. Our clients benefit from:

- Services methodology built on recognized industry standards including NIST, CIS, and ISO
- Compliance depth & breadth including PCI, HIPAA, NERC CIP, GDPR, CCPA, SOC 2, ISO 27001, DFARS 800-171, CMMC
- Multi-discipline experts provide for a broad view of client's potential vulnerabilities
- Deep security services bench and broad security services solutions provide domain expertise and consistent deliverables

Presidio Cybersecurity Practice covers a broad security services portfolio. Our highly skilled and tenured cybersecurity practitioners maintain leading industry certifications, provide thought leadership and practical industry experience. We have conducted thousands of engagements across all major industry segments. Getting started with Presidio is easy. Let's explore how we can secure your business.

Contact Presidio today: www.presidio.com